ADOA Information Security Awareness Video

Text for training video one…

Second Scenario: Judy, Judy, Judy

Scene One
Setting, Executive Office

Chad and the ISO are sitting with executive looking at newspaper headline, "High-ranking official tested positive for drug use."

Executive: Well, of course it's not true. But this article says that our agency, OUR agency records were referenced by an anonymous source. How could this have happened?

Chad: I don't know how it happened. There is only one person on my staff that has access to change those records. And I believe her when she says she had nothing to do with it.

ISO: I've been investigating this. And it looks like an inside job. Let me walk you through what I think happened.

Scene Two
Setting, Work Unit

Two office workers are at the coffee machine talking about their weekend.

Gary*:* Good morning Connie*.*

Connie: Good morning. How are you doing?

Gary: Good. How was your weekend?

Connie: I had a great weekend. How about you?

Gary: A little bit too exciting.

Connie: Oh yeah.

Gary: I helped a friend move and his truck broke down.

Connie: You're kidding.
Gary: What a mess.

Connie: Oh.

Supervisor approaches

Chad: Good morning.

Gary and Connie: Good Morning

Chad: Hey, listen, we've got that training today. We've got to figure out what to do about coverage while we're away. Why don't you grab a donut get your coffee and let's go in my office and we'll figure it out.

Gary and Connie: OK

They get their coffee and sit down at a small table in Chad's office

Chad: I talked to administration yesterday about trying to get some coverage for us today. They're sending Judy to help us out.

Gary and Connie: Oh… man

Chad: So listen, is there anything that we absolutely have to have done before we get back?

Connie: Well, I have some health forms that have to be entered in today, and that's easy. She just needs the id, the social security number, name that sort of stuff. And she can handle that, I'm pretty sure.

Chad (to Connie)**:** Okay, so you can show Judy how to sign on and do what you have to do?

Connie: Sure, I'll give her my password.

Chad (to Gary): Great. Gary, anything you need to get done before we get back?

Gary: Nope, I'm all set.

Chad: Okay good. Hey listen, I have to tell you something. Today is Judy's last day with the agency. I've been told, it's because she's unhappy about being passed over for promotion. I have also heard it is because she is late all the time. So I think we better plan for her to be late again today.

So, maybe we should come up with something in case she is.

Connie: Well, we should stay as long as we can, but if she is late, we can write her a note. We can prop the door open, and she can do what she has to do.

Chad: Can you take care of that?

Connie: Sure.

Chad: Good. Okay.

They're all ready to leave for training, but Judy still isn't there. They decide to go. Connie writes her password on a post-it note. Connie props open the door and tapes a piece of paper on it. The post-it note is on Connie's monitor..

Chad, Connie and Gary leave for the training. Show that Chad has left his computer signed on.

Scene Three

Judy arrives and sees the note. She grabs the note and reads it aloud.

Judy: "Judy, thanks for covering for us. We waited as long as we could but had to leave. Please enter health forms onto the system. Forms, file names, and password are on my desk."

(Angrily) Yeah, it's just like them to leave me THEIR work!!!

She enters the office, sits at the computer and takes a look at the post-it note with Connie's password.

Judy: *Password is "Connie." Oh that's clever, like I could not have figured out that one.*

She signs onto the health claim file using Connie's password. She pauses to help herself to snack jar on desk. She begins snooping around the system.

Judy: Well, what do we have here? I didn't know you had access to executive records. So, you think you're too good to wait for me, Connie? Well it's payback time. I'm going to help you update your files.

Judy enters false data into the record.

Judy: That's good. But, I should **share** it with someone… onto the web… YES. *(She works at the keyboard)* Here we are. (*Speaking while she's typing*) Message to: newsdesk@dailyexposure Subject: High-ranking official fails drug test. That's good, Send.

Judy: I can just see it now. 'Sir, Can you tell me why you failed the drug test? Is it true that you have long term use of recreational drugs?' Ha-ha! *That's good.*

Judy leaves Connie's desk and starts wandering around the office looking through Connie's and Gary's papers and looking at her watch, killing time. She wanders into Chad's office. She notices Chad's resume and cover letter.

Judy: Oh Chad left his machine on, good! Hmmmmm. Making a career change, Chad. Very interesting, well let me help you burn some bridges!

Judy: *(She speaks aloud to herself as she types)* Message to: headhuntersRus. Subject: Accepted other offer. Text: Dear sir, I've accepted a more generous offer from another firm, and quite frankly, I wasn't that impressed with your organization. Have a nice day, Chad.

There you go Chad. Send that right off.

Oops, I wouldn't want to leave this without password protection. Why don't I just give you a little password, here Chad. There you go, all set.

Then she adds a password to Chad's machine. She snoops around Chad's office looking through booklets and under papers. Then she walks back over to Connie's area picking up the note Connie left and reads it aloud.

Judy: Health forms, done *(checks it off on the list) She writes on the note, reading as she writes.*

"Chad, Connie and Gary: Finished work. Waited as long as I could, but had to leave. Hope you learned a lot at your training! Judy (smiley face)"

Scene Four

Back to the setting with the Chad, the Executive and ISO

Executive: *(to Chad)* I realize that your staff did not intend for this to happen. But it did and they need to fix it.
(to ISO) I want to make absolutely certain that this doesn't occur again. Can we prosecute?

ISO: Well, the State Police are investigating this. They've asked for copies of our audit trails and logs.

You know, the machines down there were pretty messed up. A password was changed, files were altered. Some of our staff couldn't even sign on. It's rare

that such a series of small incidents would come together in such a big way. When little things like this happen; like a password being left in plain view or a machine left on unattended, we might not even notice. Put all this together and we can have a serious breach of security.

I've fixed the damage, but I think this reinforces my earlier recommendation that all employees need information security training. Unless everyone knows his or her own responsibility, information security is going to continue to be a problem.

Executive: I agree; we need to take a look at the total picture and look at it now. Assemble a team to address the most critical issues and review our policies. Bring in one person from each program so that we can deal with this on an agency wide basis. And come up with a plan that we can discuss at our next Executive Staff Meeting.

ISO: I'll get right on it.

Bullets to Accompany Scenario One

- Keep passwords protected at all times. Don't share them with others or write them down.
- Do not leave your PC on and unattended.
- Be familiar with and follow policies and procedures.
- Insiders, as well as outsiders, can compromise your computer systems.
- Information should be accessible only by people who have legitimate uses for it.

Voiceover the slides:

- Use a strong password.
- It should be easy for you to remember, but long enough and complex enough to be hard to guess or "crack." Use a mix of letters and numbers or special characters. One way to create a password you can remember is to use the first letter of each word in a phrase or sentence.
- Don't store passwords on your computer or use them in automatic log-ons.
- Don't share your password with anyone and don't write it down. If you think your password has been compromised, change it.
- Don't leave your PC logged on, unattended and unprotected.

- Be familiar with and follow information security policies and procedures. They exist to protect all of us.
- Insiders, as well as outsiders can compromise your computer systems. Unfortunately, disgruntled employees as well as well-intentioned, uneducated “helpers” can be destructive.
- Information should be accessible only by people who have legitimate, job-related uses for it. We are ALL responsible for the confidentiality and protection of the information that is at the core of our business.
- Contact your Information Security Officer immediately when any breach of security or theft has occurred.
- We all must do our part to ensure good security. Follow procedures and don’t be afraid to ask questions.
- Remember--- It’s YOUR responsibility